204 – Steganography – Level 2

Team Information

Team Name: elso-ren

Results Email: [redacted]

Examination Time Frame: to

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided password protected files located in the **204_Steganography_Level2_Challenge2008** folder. Of the three files provided, identify the file that contains hidden data and extract and decode the hidden data.

Report with the exact detailed explanation of your process (software or technique) used to examine and detect the information, and then to successfully extract the information.

Total Weighted Points: 50 Total Points for correctly identifying the file containing hidden data – 150 points for extracting and decoding the hidden data. Total 200 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

Question 204: Steganography

Sysinternals 'strings' tool was used to provide unicode data.

$ strings.exe -u File3.jpg

mirage.bmp

$ hachoir-subfile --offset=168782 File3.jpg .

[+] Start search on 218528 bytes (213.4 KB)

[+] File at 168782 size=218526 (213.4 KB): Compressed archive in 7z format => ./file-0001.7z

[+] End of search -- offset=387310 (378.2 KB)

Hex editor

29340 -> end of file

Hachoir was used to search for subfile (or embedded files) within files. A file in 7z format was found. this 7z file was carved out of the jpg file by using hachoir to identify the starting offset of this file as well as the size. A hex editor was used to move to the offset 29340 and copy that data to the end of the file. This data was then copy to a new file and was provided the extension'.7z' This file was unzipped and contained the file mirage.bmp.